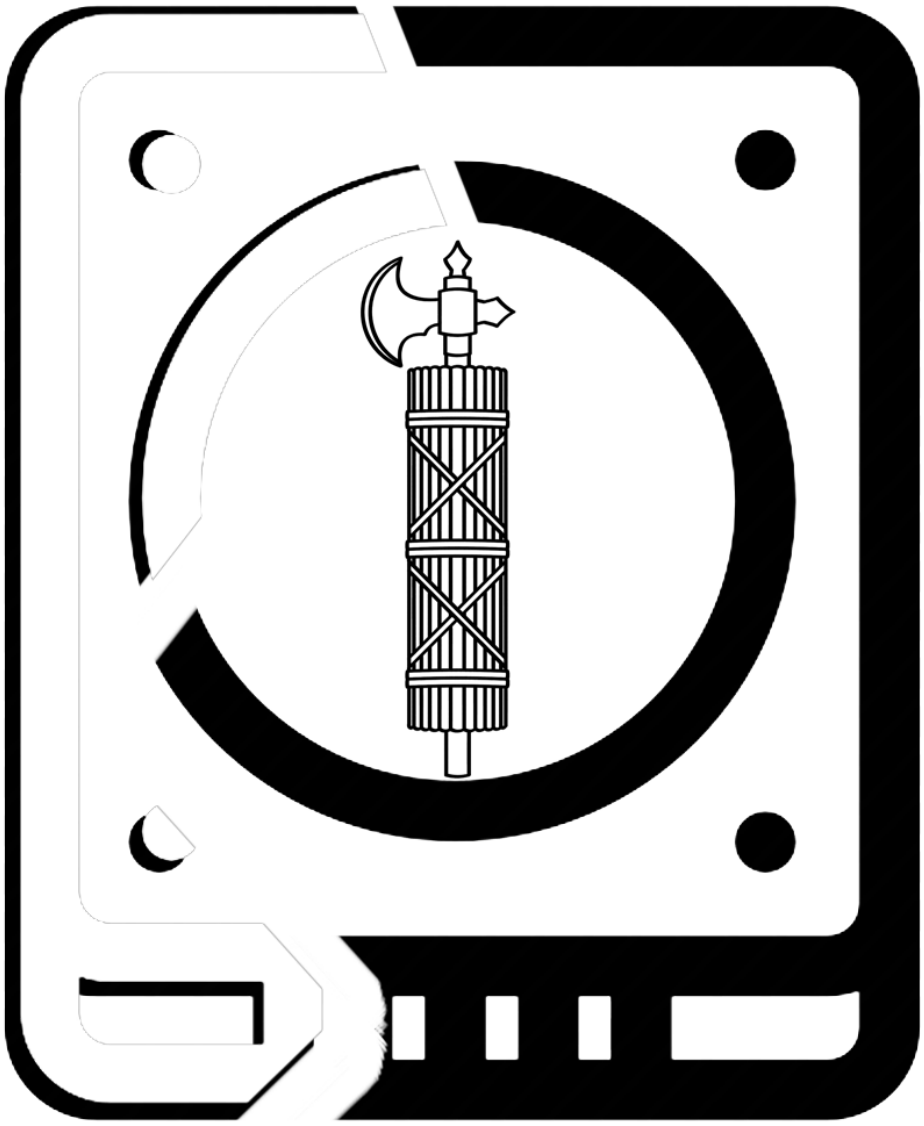
Archival Data Storage

Net Fascist's Guide



Data Protection In The Age of

INTERNET MARXISM

Old Net Principles:
The Anarchists Have Become Fascists

During the early days of Net use, the Wild West of the internet was characterized with ultimate freedom. Freedom to share what you wanted, freedom to go where you wanted, and ultimately to say what you wanted to.

It was the time of total creativity, and by the measure of its difficulty of usage, it was a domain of the White man, and those few other groups of people smart enough to operate it.

Rakim, Oakland: "See, computers are racist because they make them too hard to use. They need to make them easy like TV, so people in the community can have good jobs. Computers are made by whites and Chinese, and they don't like it when we try to get ahead.

The invention of the internet was one of the most terrifying things to the Marxist, who hates truth and freedom, because it allowed for uncensored access to information. They had censored every textbook and every pamphlet already in print, but this new frontier was completely outside of their reach. Most importantly, circles where White men didn't have to conform to the quickly changing landscape of Marxist domination.

Now, computers have become easy like TV. The Marxist saw the great value of giving the internet to those who didn't understand it, and have created a generation of drones with the smartphone to their superior united disinformation and censorship efforts.

Like children, we did not understand the great freedom afforded to us, we were disunited anarchists, small individual pieces trying to enjoy the freedom of the early net only caring about our little slice of freedom, shirking responsibility. We did not appreciate the power of unification and we have lost much ground to those Marxists who have now come to dominate the internet like they had in realspace politics. The tide is changing however. This is where the frontier begins anew.

Table of Contents:

Physical Storage

All data is stored on a physical device somewhere. Every byte and file type lives on a physical spot as data, regardless of format (PNG, JPG, AVI, MP3, etc). Even data that is not physically on your device but in a cloud is hosted off-site on a physical storage device in a warehouse whether owned by Google, Archive.org, or otherwise.

These storage devices each have different methods of holding data, and have their own pro's and cons. Additionally, there is a question of "hot" or "cold" storage, which affect these devices differently. The primary storage devices are as follows:

HDD: Hard Drives with spinning discs. These are magnetized disc drives that have physical moving parts. They are slower than SDD when processing data actively. They utilize a physical disc and bearing grease to spin them. This is fixed disk memory
Includes HDD Drives, DVD/CD Rom.

SDD: Solid State Drives. These are a series of switches that store electrons and the data is housed in these little switches. They operate much faster than HDD and have no moving parts but are more susceptible to data loss when cold. This is flashed memory.
Includes SDD Drives, Flash Drives, SD Cards

Dino-Ware: Older computers will utilize HDD technology, but will be excluded from this guide because of their requirement for outdated and often times difficult to find hardware needed to read them.
Includes Mainly Floppy Disk Technology.

Hot and Cold Storage

Data is either hot or cold depending on whether it is actively being used on a computer, and this will affect its data integrity capabilities. When a device is plugged in it becomes hot, when it is not it is cold. Cold Storage refers to a device that is going to be unused for extended periods of time.

Physical Device Options

Data Rot: The arch-enemy of archivists. This is data that has become corrupted simply by being unused. When data sits on a physical device unused, it decays just like anything else. There are ways to mitigate this issue however. While some overstate the danger and likelihood of it, it is indeed real in some measure. **Data Rot** occurs in both Hot and Cold devices, but adores data in Cold Storage

HDD Drives: HDD's will have much better Cold Storage capabilities than SDD Drives because of the physical imprint on the discs, but are still susceptible to Data Rot. Additionally, they should be plugged in and spun routinely, the bearing grease between the discs will dry out if they are unused. Unused HDD's, even if the data is still safe and whole on the discs, may fail to be accessible simply because the discs do not spin.

SDD Drives: SDD's have very bad records in Cold Storage, but there is no telling exactly when Data Rot will set in on an unused SDD. It could be weeks, months, or years; it can also vary in severity. Some USB drives and SD Cards (which are all SDD) can last a decade and have whole, usable data when plugged in, but this is absolutely not recommended. In Hot Storage, the integrity of files should be relatively safe, and the speed of SDD makes them the preferred drive for active use.

Optical Discs: This is a form of HDD Technology but care should be exercised when using them and what type is being used. Regular DVD-R and DVD-RW discs are suseptible to a particular type of Data Rot called **Disc Rot** where the chemicals used in burning a DVD disc begin to melt away after a number of years and will appear as see-through holes in the disc. This is unpreventable. These types of discs should be distinguished however from M-Disc Archival type BDR type Optical Discs which use a different, much more robust technology when burning.

Long Term Cold Storage

HDD Drives: can be used for Cold Storage, but spin the disc at least once a year to make sure it is not dried out.
Seagate makes an 8TB HDD Archival drive which is recommended by Data Hoarders

SDD Drives: Semi-Anually, devices should be plugged in, and possibly even refreshed by copying the data off and back onto the drive to maintain integrity of files.

DVD/CD: This technology is outdated, and is not recommended.

M-Disc Archival BDR: This is utilized by the US D.O.D. and data is directly engraved on the discs as opposed to being written. This makes them resistant to environmental factors and is one of the top recommended methods of long term Cold Storage.

Folder/File Compression

Files and their Folder Directories can be merged together into an **Archival Directory File** through the utilization of Softwares like Winrar, 7Zip, and Freearc. Entire folders and all of their contents can be merged down into a single shareable file than can then be uploaded to shared clouds, or sent through emails so that the recipient only has to keep track of a single Archival File. This is also useful for practical usage in sharing folders of files for work (like a dozen word documents and so on). These files have extensions like .rar, .zip, .7zp, .tar, or even .iso.

Many of these programs also offer the option to password protect these **Archive Directory Files** so that the recipient must enter a password to open the file and extract its contents, making it a more secure form of sharing protected data.

I will not include a step-by-step guide on how these programs work, only that I recommend 7Zip over other programs, and will give a short word about it in the Compression Section

Compression

These **Archival Directory Files** can be compressed so that they take up less size during data transfers, using dictionary and word sizes. This can mean a Folder that is 1GB can be reduced to half or even less of its original size in an Archival File depending on how much it is compressed.

A word of warning: Archival File size is dependent on how large Dictionary and Word Sizes are, but the larger they are the more likely they are to become corrupted. If a single piece of a large compression dictionary is corrupted, the entire file is unrecoverable (unless there is a parity backup). Uncompressed Files in Archival Format are safest for Cold Storage, but will take up more space.

To prepare a folder/file for an Archive:

1) Right click on the folder/file, hover over 7-Zip and press Add To Archive
2) Choose extension, Compression Level, and Method. LZMA is for higher compression, use level 0 for simply creating an Uncompressed file.
3) Choose Dictionary and Word Size.
4) You will see an option for “Encryption” on the right side. This is where you can assign a password for opening the Archival File.

Archive Safety

Compressed Data is naturally more at risk for corruption than uncompressed data. In a Jpeg, a misaligned byte can result in a small discoloration. But in a Jpeg that is in an Archival File, a misaligned byte will result in a picture that cannot be opened or viewed.

There are ways to mitigate this risk, the foremost being the creation of a parity file, which is a redundancy file that can be used to repair broken files of all kinds, whether they are videos, pictures, or Archival Files. Parity files were commonly used in the early net to repair broken Rar files that were sent through Usenets and often became corrupted.

The more broken a file is, the more parity blocks will be needed to repair it. Parity also works by hitting random blocks of data inside a file. The more redundancy a parity file has, the more likely it is to hit any given corrupt byte in a file. Therefore, more sensitive and important files should be given higher redundancy parity files. Of course, the more redundancy, the larger the parity file. These can also be compressed in Zip files, but remember that it will again just expose them to the same risks as the file you are keeping them to repair with.

QuickPar

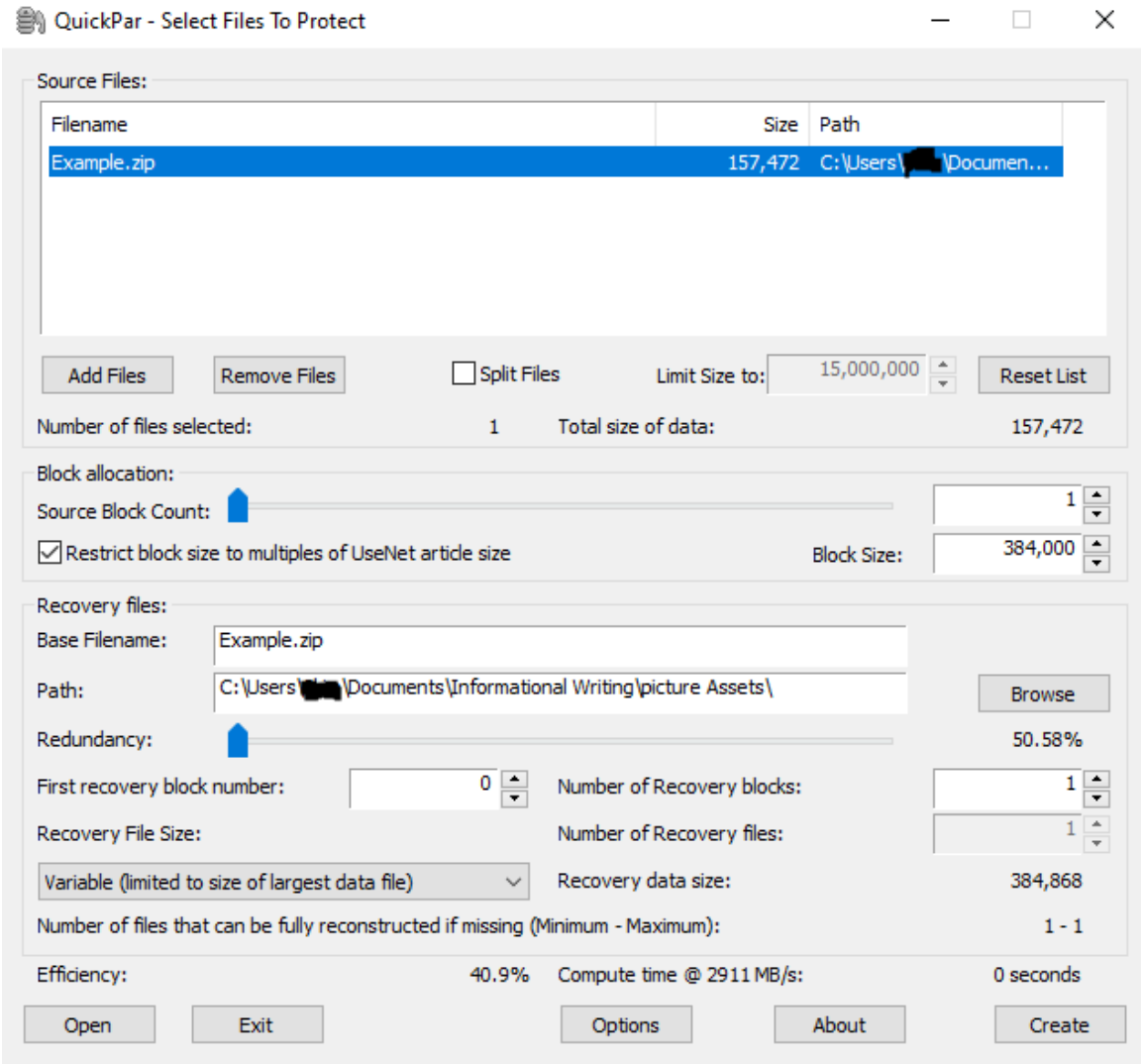
Quickpar is an old Parity creation software which creates PR2 files for use in repairing any file type. The next page will detail the creation and use of this program.

Quickpar Guide

Creating Parity Repair Files: The first step is to click Add Files, from there, select your zip or other file type that you will be creating a Parity Repair file for.

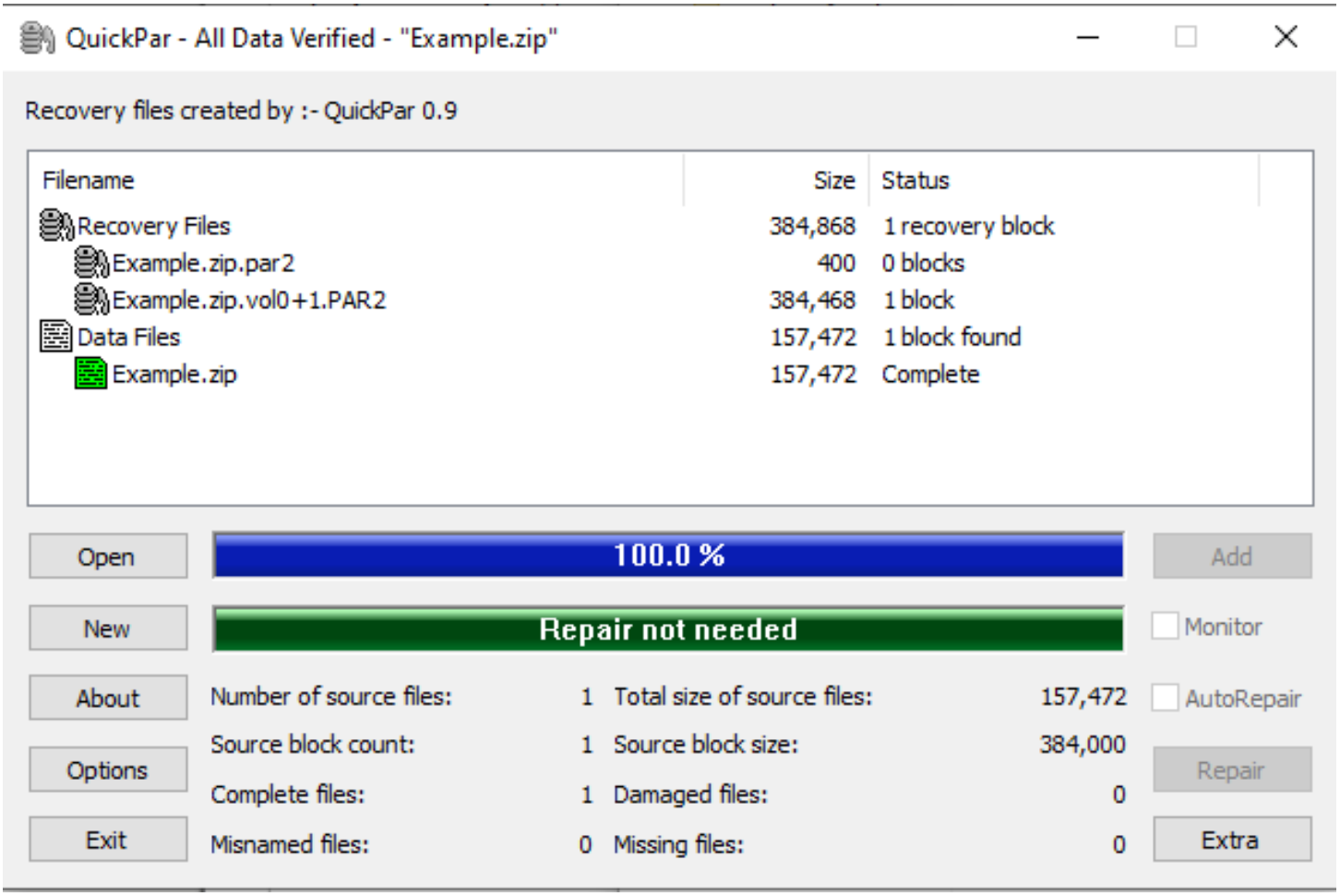
2) Adjust your settings. I leave the first block allocation section alone, but then I will adjust the Redundancy slider depending on the importance of the file. The more redundancy the safer the files will be, but it will create more blocks of Parity data that take up space. The more redundancy the more likely in big files one of the Parity files will have a "hit" on a missing patch of data during the event of corruption.

3) Click create when finished. It will spit out a PR2 file and blocks of Parity files with it. You will need to keep all of these for a future repair.



Quickpar Guide

Repairing Files with PR2: The first step is to make sure all of your PR2 files are in the same current directory of the file you are repairing. They should all be located in the same folder.
2) open the program to the main window, and click Open, located at the bottom of the window.
3) Select the main PR2 file, it should have the shortest name.
4) Another window will open up automatically, telling you whether a repair is needed, and if so how many blocks are required. If the missing bytes are located in any of the PR2 files, it will give you the option for repairing the corruption or the missing files. If however the corruption is in a block which the PR2's did not cover, you will not be able to repair the file. Smaller files will require more redundancy naturally than larger files. Gauge how valuable the file is to you, as a 100% redundancy will be a 1:1 in file size, but anything greater than 50% is almost always unnecessary



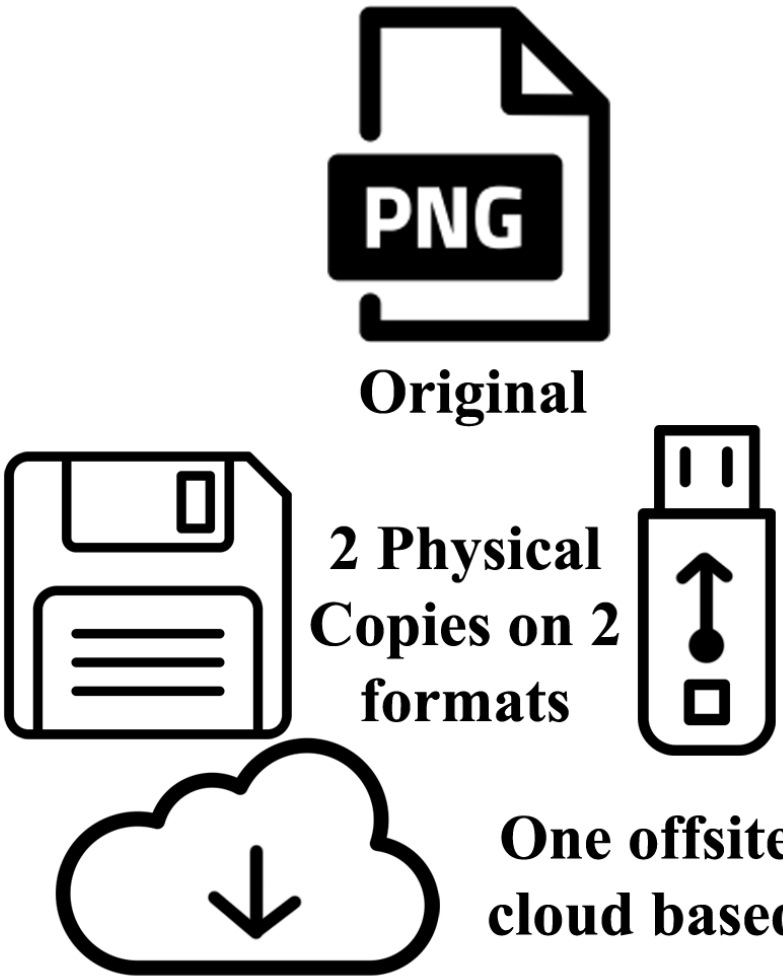
3-2-1 Rule

Ultimately, for data you absolutely cannot risk losing, you should follow the 3-2-1 Rule:

3 Copies of the Data.

2 Copies are on a different format as the original and from each other.

1 copy is stored off site on a cloud or web service to protect against disasters like fire.



Online Options

Regardless of what online companies tell you, they will not protect your data. Much like a radio broadcast, anyone who is around and on your channel will hear your message, the encryption is what protects the message from falling into hands that you'd rather your message not fall into.

Nothing is stopping companies from handing over data to the government, or other operations if they are asked. Never place your data into a network-based server **unless you don't care if whatever is inside of it gets leaked**, **or if you believe it can't be traced back to you.**

Obviously in the latter case things can be done to increase your anonymity when uploading files, such as bringing the data in on a Flash Drive and using public library computers for uploading, using someone else's computer and credentials, etc.

Here are some places for online sharing:

Google Drive: Every account on Google gives 15GB of free storage. With Archival File Password protection and direct sharing of links to files, it is unlikely you will catch heat for an upload if you are smart about data (and it getting flagged by bots) and compression. Links are not publicly broadcasted.

Archive.org: Use this site if you are uploading files you want any user to easily find if they search for it. It is a community based cloud archive.

Anonfiles: A very slow cloud site that will spit out a link to your file once uploaded. No clue on how long it remains up however.

Catbox.moe: See above. Usually used for sharing stuff on the Chan's.

We.tl: A favorite of Pirates. Links are share-only and files expire after 7 days. It is likely your files remain on their servers longer however, so keep it in mind.

Covert Information Exchange

If you want to be a real internet sheister, there are several methods of covert communication and obscurity options for sharing links to online archives, or sending of messages. Here are some options.

Base64 Encoding: Base64 is a method of encoding text in a sentence, and is often used by pirates to hide links when they are sharing information back and forth on forums. You can encode a link, then add puzzles into the new text, encode it again, and repeat this as many times as you want. As the person decodes the message, they will have to reverse what ever steps you have taken to get the original link. I'll leave you this one for your amusement:

WVVoU01HTklUVFpNZVRrMVlqTldNR1FvWkdWc1pYUmxJSFJvWlNCMFpYaChyZXBs
YWNlIHRoaXMgYW5kIHBhcmFudGhlc2lzIHdpdGggNXgwKUlHRnVaQ0J3WVhKaGJuUm
9aWE5wY3lsVE5XbGFVemxyVlZoak1HUjZiRmhhTVdocVZWRTlQUT09

Hex Coding and App-ending: Through the use of Hex Editors like HXD, you can directly inject messages like links or text into files. If the file format is one that doesn't rely on tight compression, you can insert this into most anywhere in the file and the file will remain intact. If the recipient knows what line of code to look for, there the message will arrive. That being said, your links and text can be thrown directly onto the end of a file's code and almost never affect it's integrity. This has been tested with pictures sent through discord and telegram viewing the original image and saving it, then opening it in HXD, the messages were fully intact.

Sending Broken Files: Many different types of file formats will simply not work if a chunk of data is ripped from them. Simply open the file in a Hex Editor, cut a chunk of data out and mark which block it was ripped from. Send that block to the recipients with the location. The broken file is posted online on a cloud. They can then reinject the code and repair the file, allowing them and them alone to view the intact contents.

Data Organization Tips

As an avid Archivist, I can assure you that meticulous organization in the beginning pays dividends as you archive grows. My political archive is organized by

Source (internet, real life, organization)> topic>sub-topic>then whether it is an Article (PDF) video, or picture. An example of one of my file paths is: C:\Internet\interesting news\Anarcho Tyranny\Articles

When saving an article online, a very useful trick is to right click the page, select print, and then when choosing a printer select “save as PDF”. This will allow you to safe the article, and number the pages you want saved to cut out comments frequently found on sites like Dailymirror or CNN. It is also a good idea to create a backup on Archive.today or Archive.is for other Archivists to access at a later date.

When saving your story, you should always give a date to your file name. This is paramount. Dates can be added at the end or at the beginning, if you add them at the beginning it may be better for organizational purposes. Because computers cannot name files with a “/” in its name, simply use the format month-day-year e.g. 7-4-23.

Additionally Archive.today can help you bypass paywalls on some websites if you don’t know how to remove them yourself through HTML editing.

LAN and E-LAN Computer Communications

LAN (local area networking) is the fastest and most secure method of connecting two computers for transfer of information, or simply playing games for that matter. The simplest way to accomplish this is connecting two computers with an ethernet cable in their network ports and opening a network neighborhood (now called “network discovery” for fags of the 21st century). From there, folders can become discoverable for computers sharing any connections.

There is a such thing as E-LAN as well, creating LAN connections over small network neighborhoods connected through third parties. One genius from Russia in 2004 created a program called Hamachi, which simulates a local area network, assigning a VPN to a computer and allowing other computers to connect to their E-LAN VPN network. Obviously, this is not as secure as a real LAN network, but it is another layer of obscurity and offers some really good options for communications cutting out middlemen. No physical ethernet cables required.

Using the IP address Hamachi gives you through your VPN, you can open closed IRC channels, closed voice chat channels, closed file sharing, and even closed gaming servers available only to those in your network neighborhood through the E-LAN connection.

To summarize what someone would need to do to tap into your line when using this method, they would have to:

1) Have an interest in you because you put a target on your back
2) Know you are using E-LAN to communicate
3) Know which E-LAN service you are using.
4) Know which program you are using to communicate over the E-LAN
5) Know the VPN IP you are using, and the password of the server you are hosing over the program on the E-LAN connetion (IRC etc).
6) Tap in without you knowing via IRC server Admin metrics.

Secure Communication and Methods of Contact

Nothing these days is 100% secure. With enough time and energy, and with enemies that you have pissed off enough, skilled people will be able to find your data and the one who posted it. All you are doing is making it more difficult. Think of being a Net Fascist in the age of Internet Marxism like driving 120 mph on the highway.

You can either go balls to the wall with bald tires and take your seatbelt off, or you can swap on some good tires, weld in a roll cage, put on your helmet, and buckle up into your race harness.

The following are some good E-LAN programs for more secure forms of communication that let you talk without utilizing a public server open and available to anyone:

Unreal IRC: An oldschool program that lets Admins know who is in their server, post MOTD's, have a server password. The whole 9 yards of early net days. Server is only up when a host turns on the server on their computer, and goes down when he takes it down.

Mumble: a personal favorite for communication over E-LAN. Encrypted voice chat with password protection and some very light file sharing capabilities. Server is only up when the host runs Murmur (the server client), and goes down when Murmur is closed.

LAN Games: Sounds a bit weird at first glance, but hosting a game of CS 1.6 on a LAN connection is a very wild and unconventional way of communicating and offers both text and voice chat capabilities. Depending on your know-how, it also offers file sharing capabilities through the downloading of server data to client-side computers that are connecting.

Thanks!

Hail Christ, Hail Victory!